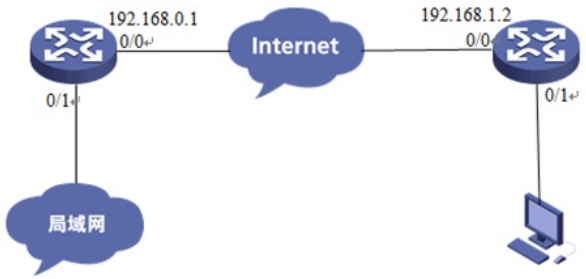
WIN7电脑使用INode客户端进行L2tp over ipsec拨号建立VPN

L2TP IPSec 刘嘉炜 2015-12-30 发表

解决L2tp over ipsec组网中，WIN 7电脑不支持ipsec tunnel模式建立IPSEC隧道问题。



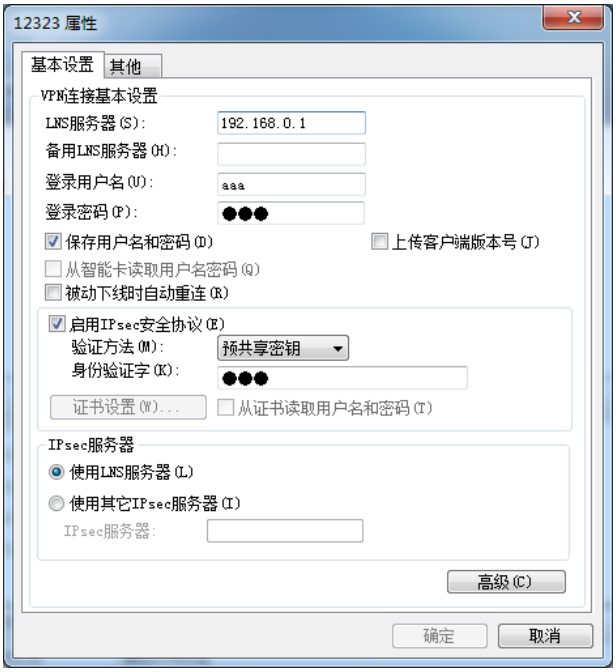
实验配置:

```
l2tp enable                                  \\开启L2TP功能
#
 ike local-name a                            \\指定本端的IP地址
#
domain system
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
 ip pool 1 1.1.1.1 1.1.1.10                  \\创建地址池
#
ike proposal 1
 encryption-algorithm 3des-cbc
 dh group2
#
ike peer 1
 exchange-mode aggressive
 pre-shared-key cipher $c$3$kPhZOqmZui7ArDAzv53x/5pqQxim9w==
 id-type name
 remote-name b
 local-address 192.168.0.1
 local-name a
 nat traversal
#
ipsec transform-set 1
 encapsulation-mode tunnel
 transform esp
 esp authentication-algorithm sha1
 esp encryption-algorithm 3des
#
ipsec policy-template 1 1
 ike-peer 1
 transform-set 1
#
ipsec policy 2 1 isakmp template 1
#
local-user aaa                               \\建立本地用户
 password cipher $c$3$6YznH80JQRGeKUN8iV3JkOA0J8SKlA==
 service-type ppp
#
l2tp-group 1
 undo tunnel authentication
 allow l2tp virtual-template 1
 tunnel name 123
#
```

```
interface Virtual-Template1
 ppp authentication-mode chap
 remote address pool 1
 ip address 1.1.1.1 255.255.255.0
#
interface LoopBack0                          \\配置loopback口模拟内网
 ip address 2.2.2.1 255.255.255.255
#
interface GigabitEthernet0/0
ip address 192.168.0.1 255.255.255.0
ipsec policy 2
#
 ip route-static 0.0.0.0 0.0.0.0 Virtual-Template1
```

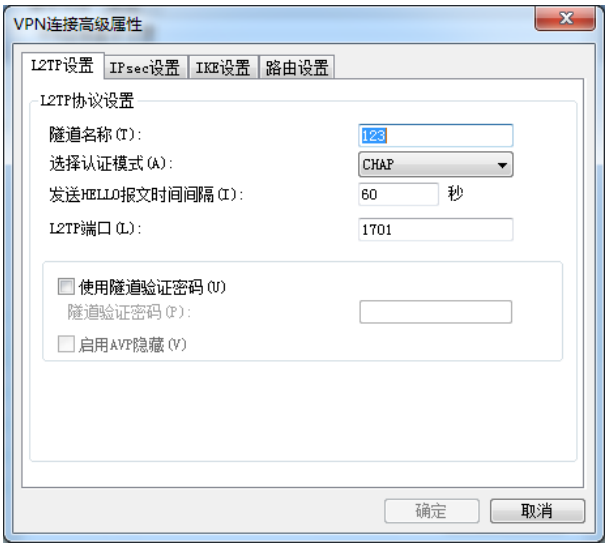
INode客户端的配置：

1、首先下载iNode PC 5.2 (E0408)这个版本软件，目前最新INode软件已经取消了L2TP功能。

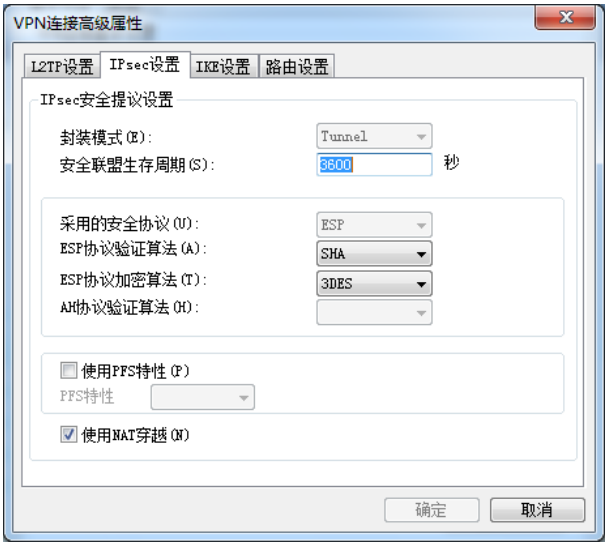


LNS地址对应提供L2TP服务器的IP地址，登录用户名密码为L2TP的用户名和密码。IPSEC与共享密码为IKE中设置的密匙。

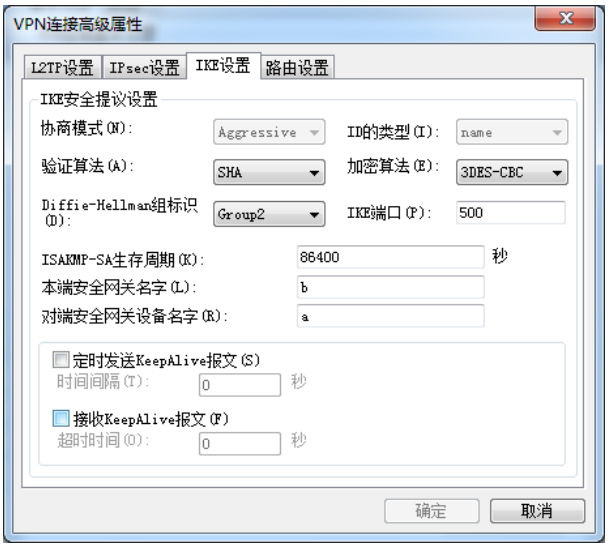
2、点击高级设置后选择L2TP模式为“CHAP”的验证方式。



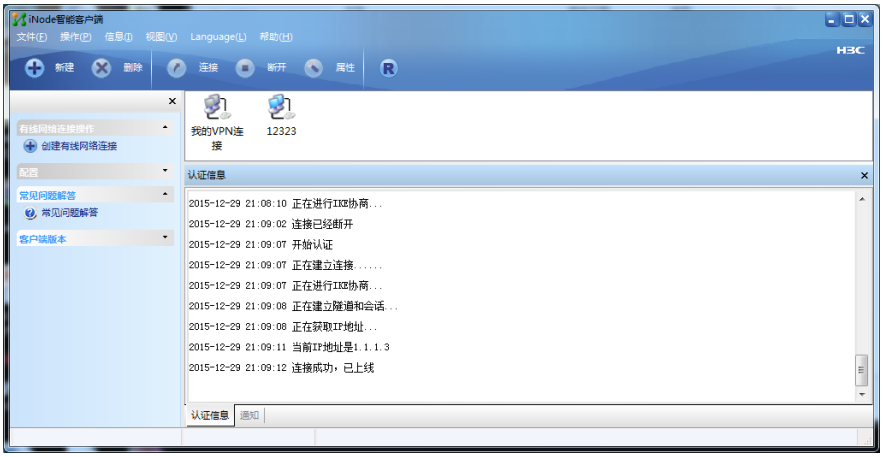
3、设置IPSEC的加密和验证算法



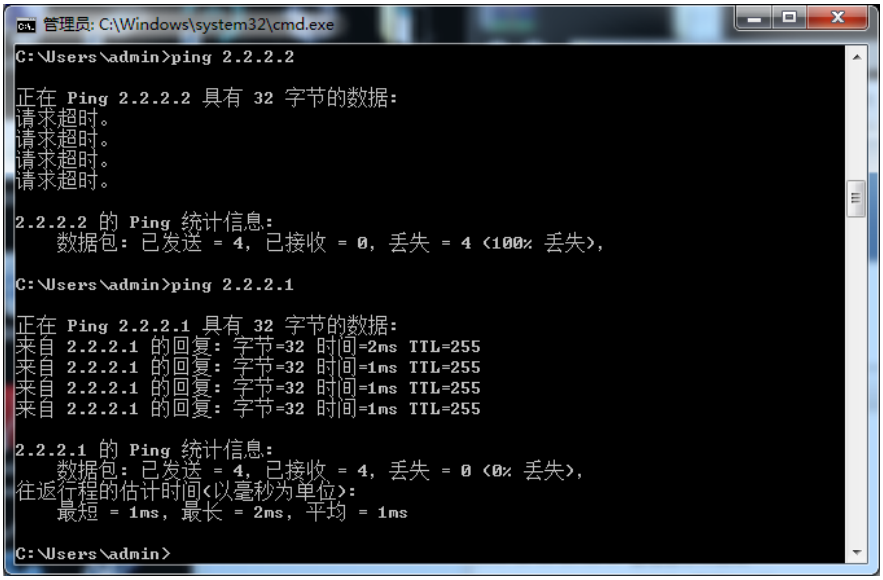
4、设置IKE协商参数



5、进行L2TP拨号



6、设置成功后查看路由，测试ping对端内网地址



查看设备侧的SA信息：

```
display ike sa
  total phase-1 SAs: 1
  connection-id  peer                 flag       phase   doi
 ----------------------------------------------------------------------
    28          192.168.1.2          RD         1       IPSEC
    29          192.168.1.2          RD         2       IPSEC
 flag meaning
 RD--READY ST--STAYALIVE RL--REPLACED FD--FADING TO--TIMEOUT RK--REKEY
dis
display ipsec sa
================================
Interface: GigabitEthernet0/0
  path MTU: 1500
================================
 ----------------------------
 IPsec policy name: "1"
 sequence number: 1
 acl version: None
 mode: template
 ----------------------------
  PFS: N, DH group: none
  inside VRF:
  tunnel:
     local  address: 192.168.0.1
     remote address: 192.168.1.2
  flow:
     sour addr: 192.168.0.1/255.255.255.255  port: 1701  protocol: UDP
     dest addr: 192.168.1.2/255.255.255.255  port: 0  protocol: UDP

  [inbound ESP SAs]
    spi: 0x2901DF91(687988625)
    transform: ESP-ENCRYPT-3DES ESP-AUTH-SHA1
    in use setting: Tunnel
    connection id: 23
    sa duration (kilobytes/sec): 1843200/3600
    sa remaining duration (kilobytes/sec): 1843196/3586
    anti-replay detection: Enabled
     anti-replay window size(counter based): 32
    udp encapsulation used for nat traversal: Y

  [outbound ESP SAs]
    spi: 0x6AC7C993(1791478163)
    transform: ESP-ENCRYPT-3DES ESP-AUTH-SHA1
    in use setting: Tunnel
    connection id: 24
```

sa duration (kilobytes/sec): 1843200/3600
sa remaining duration (kilobytes/sec): 1843199/3586
anti-replay detection: Enabled
  anti-replay window size(counter based): 32
udp encapsulation used for nat traversal: Y

1、 L2tp over ipsec隧道，并非我司设备不支持tunnel模式建立隧道，而是Windows客户端无法支持，在这种情况下最好使用Inode客户端去认证。
2、 使用Transport模式建立的L2TP over ipsec 只能在内网搭建，因为transport模式限制不能穿透公网，所以此配置完全符合客户实际使用环境。